機械安全と機能安全への取組み ── Total Safety ──

特集

小塙 明比古（こはなわ　あきひこ）　**長谷川 正美**（はせがわ　まさみ）

1　まえがき

最近，機械装置やプラントで重大な事故が相次いでおり安全・安心の向上へ社会的関心が高まっている。安全・安心の構築には，危険（リスク）発生の予測，設備の予防保全，プラントのセキュリティ，システム上のデータの電子記録など広範囲な応用技術が必要である。一方，設備設計やシステム設計の段階で安全を確保する新しい手法が，機械安全や機能安全として体系的に規格化されてきている。

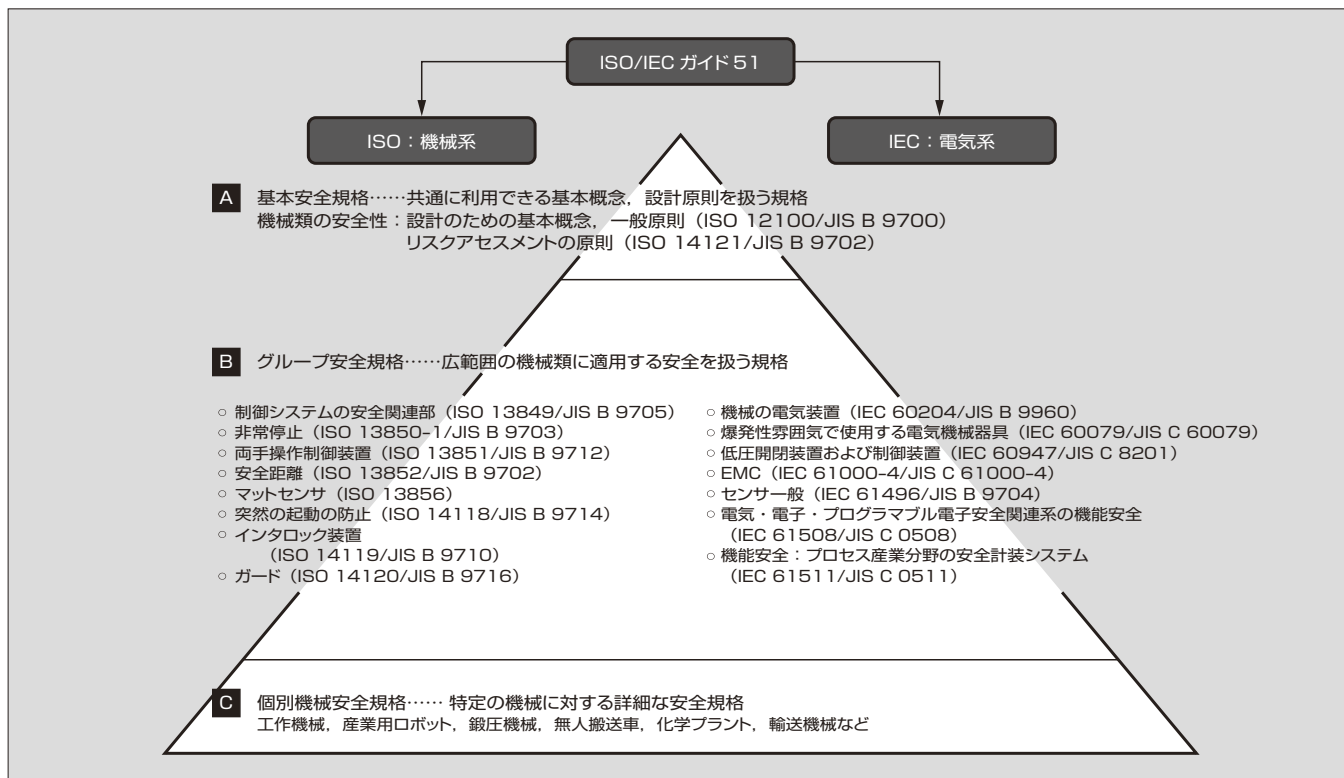
本稿では，現在生産現場の設備やシステムに取り入れられてきている新しい安全構築の手法を概説するとともに，富士電機の安全への取組みを紹介する。

2　安全規格の内外動向

2.1　安全規格の整備状況

欧州では，安全性能に関する基本概念や設計原則を規定する安全規格が広く活用されてきた。これを背景にISO/IEC ガイド 51 が発布され[1]，国際規格 ISO 12100（機械類の安全性－基本概念，設計のための一般原則）が発行され，かつこの規格を頂点として，**図 1** に示す体系的な安全規格が構築されている。今後，個別の機械やシステムの安全規格がさらに充実されると予測される。

わが国では，WTO/TBT 協定にのっとり**図 1** の国際規格体系を受け入れ，ほぼ同じ体系で JIS を制定して安全規格を整備してきた。この動きと並行して国内法では，2006

図 1　安全規格の体系

小塙 明比古

低圧遮断器の開発設計，低圧機器・システム全般の商品企画に従事。現在，富士電機機器制御株式会社生産本部技師長。電気学会会員，電気設備学会会員。

長谷川 正美

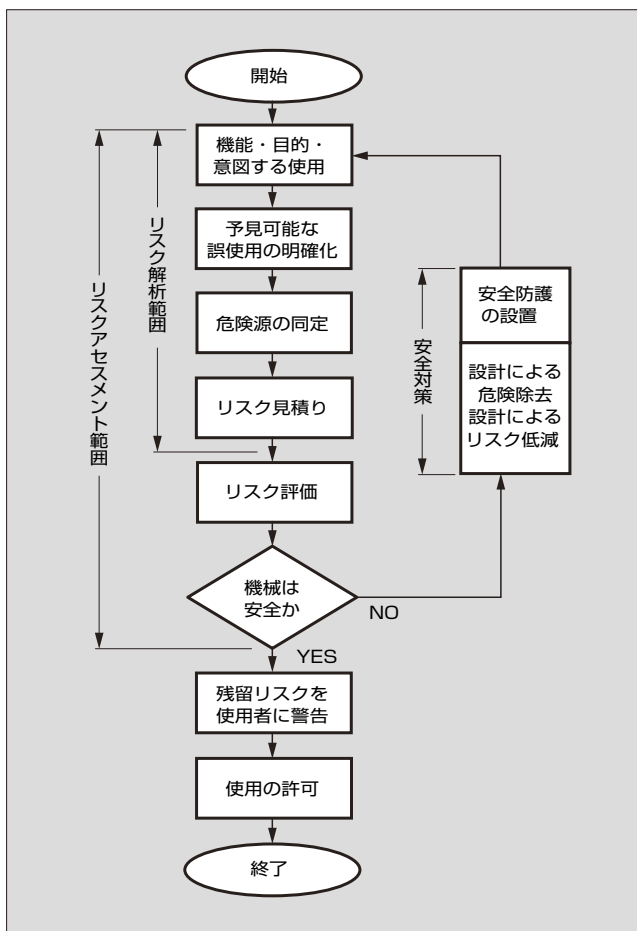
安全計装システムの開発・設計業務に従事。現在，富士電機システムズ株式会社制御システム本部情報・制御センター制御システム部課長。計測自動制御学会会員。

図 2　改正労働安全衛生法

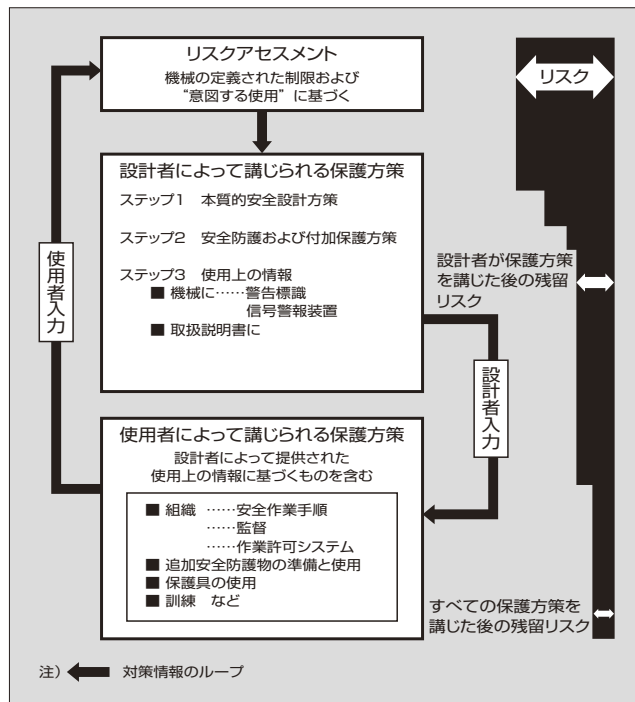
改正労働安全衛生法 11 のポイント

1	長時間労働者への医師による面接指導の実施
2	特殊健康診断結果の労働者への通知
3	危険性・有害性などの調査および必要な措置の実施
4	認定事業者に対する計画届けの免除
5	安全管理者の資格要件の見通し
6	安全衛生管理体制の強化
7	製造業の元請事業者による作業間の連絡調整の実施
8	化学設備の清掃などの作業の注文者による文章などの交付
9	化学物質などの表示・文書交付制度の改善
10	有害物ばく露作業報告の創設
11	免許・技能講習制度の見直し

対象：安全管理者の設置が義務付けられた全事業所

図 3　リスクアセスメントと安全対策

年 4 月に労働安全衛生法が改正され，「危険性・有害性等調査および必要な措置の実施」が法制化された。これにより，機械設備の新規導入や変更時，または作業方法や手順の変更時には，リスクアセスメントの実施が義務づけられた（**図 2**）。

従来，わが国は“安全は現場管理による”との考えに象徴されるように管理責任の意味合いが強かった。新しいリスクアセスメントの概念（ISO 14121）は，**図 3** に示す

図 4　ISO 12100 基本概念

手順を用いて，危険源が事故に発展するプロセスを精査し，危険源と事故の関係を遮断する手段として確立された。すなわち“安全は危険源の管理による”ことが新しい国際的な安全規格の動向となっている。

2.2　設計者の観点によるリスク低減プロセス

ISO 12100/JIS B9700 では，安全設備・システムの一般設計原則として“設計者によって講じられる保護方策”と“使用者によって講じられる保護方策”が相互にフィードバックするサイクルを規定している。**図 4** に示すようにリスクアセスメントに対応した本質安全設計を中心に残留リスクを低減する方法は“設備に安全を造り込む”ことと理解される。すなわち，“機械は故障するもの，人は間違いを犯すもの”が前提となっている。このプロセスでは，危険源の同定，適切な対応策の適用など高い技術力が必要であり，富士電機では，この技術を持つアセッサーを養成中である。

3　Total Safety の考え方

現在の生産現場は，機械装置，それらの駆動装置，全体のコントローラ，反応プロセスを含む計装などが複雑に配置されている。しかも，安全系は標準系の一部として形成される。したがって，生産現場全体の安全系を構築する場合，性格の異なる安全基準を理解して適用しなければならず容易でない。しかも，従来このような生産現場の安全系は，労働安全衛生部門が統括している場合が多く新しい安全基準の適用の推進は，今後の課題となっている。富士電機では**図 5** に示すように，機械安全・制御安全・機能安全のすべてを統一し，顧客へのコンサルティングによる

特集

安全ソリューションの提供を目指している。これが Total Safety の考え方である。

4　機械安全への取組み

FA 分野において，安全系を構築する場合，機械装置の運転に伴って危険な状況が生ずるシステムでは，基本的には“止める安全”を原則とすると言われる。具体的には，機械装置の危険源への侵入を直接ガードする方法に加えて，

図 5　Total Safety コンセプト

図 6　機械の電気装置の安全規格の対象項目

物理的環境
警告標識および略号
技術文書
システム／セル制御装置
電源断路機器
感電保護
装置の保護
接地（PE）端子
保護ボンディング回路
制御回路および制御機能
非常停止機能
制御装置
付属品および照明
電源
接地端子
電線およびケーブル
配線
試験
非常停止機器
電動機の制御装置
プログラマブルコントローラ
操作盤
入出力インタフェース
安全防護物および警報機器
電動機およびトランスデューサ
機械アクチュエータおよびセンサ
機械装置
白ヌキ部分
安全規格の対象

図 7　制御盤の安全システム

AS-i Safety システム
非常停止スイッチやセーフティライトカーテン，安全ドアスイッチその他のセーフティセンサからの安全入力をセーフティリレーに代わり論理処理し安全な停止を行う E/E/PE 機器

電源引込用配線用遮断器
○ 断路（アイソレーション）機能付遮断器
○ ロック機能付き操作ハンドル

配線用遮断器，マニュアルモータスタータ，電磁接触器，サーマルリレー
○ 過電流保護
○ 電動機の過負荷保護
○ 欠相保護

Safety PDS*1
可変速電気駆動システムについては，個別製品規格制定にあわせた情報の追加予定

電源断停止回路用電磁接触器
○ 安全カテゴリ 3 以上達成には冗長化
○ 安全カテゴリ 2 以上達成には安全開離機能接点（ミラーコンタクト）

FS*2 PLC
機能安全 PLC については，個別製品規格制定にあわせた情報の追加予定

非常停止用押しボタンスイッチ
○ 直接開路動作機能接点
○ トリガーアクション機構

*1：PDS（Power Drive System）
*2：FS（Functional Safety）

表１　機械の電気装置の安全要求事項と対応

IEC 60204-1・JIS B 9960-1要求事項	安全規格対応製品	備　考
4.2項　装置の選択	富士グローバル規格認証製品 配線用遮断器，電磁接触器，押しボタンスイッチなど	－
5.3項　電源断路機器	G-TWINブレーカ・ELB 外部操作ハンドル	アイソレーション適合 IEC 60947-2適合
6.2項　直接断路機器	フィンガープロテクション構造 （各種機器に搭載）	保護等級 IP20
7.2項　過電流保護	G-TWINブレーカ・ELB マニュアルモータスタータ	過電流保護機器間の協調
7.3項　電動機の過負荷保護	マニュアルモータスタータ 電磁接触器，サーマルリレー	過負荷/保護機器との協調
9.2項　制御機能	非常停止機能にカテゴリ0の停止を使用する場合は，ハードワイヤによる電気機械部品だけで構成しなければならない。	IEC改訂（2005年10月。JIS改訂中）によりハードワイヤ条項は削除され，電気・電子・プログラマブル電子機器の使用が可能になった。
9.4項　故障時の制御機能	電磁接触器	安全開離機能接点（ミラーコンタクト） IEC 60947-4-1付属書F
10.7項　非常停止用機器	非常停止用コマンドスイッチ	直接開路動作機能 IEC 60947-5-1付属書K適合 IEC 60947-5-5適合 セーフティトリガーアクション機能 ISO 13850適合
12.3項　エンクロージャの保護等級	コマンドスイッチ：IP65 外部操作ハンドル：IP54 （配線用遮断器用）	一般産業用エンクロージャの保護等級の要求 IP32，IP43，IP54

注）カテゴリ0 ： 機械アクチュエータを直接遮断する停止

機械の電気装置（IEC 60204/JIS B9960-1）の安全規格の適用が中心となる。**図６**に機械の電気装置の安全規格の対象項目を示す。

4.1　機械装置システムの安全に関する規格

機械装置システムの安全に関する上位規格には ISO 13849-1，IEC 60204-1，IEC 61508 の三つがある。

(1)　ISO 13849-1

機械制御システムの安全関連部の一般設計原則で危険度と安全カテゴリーの分類を示している。2006 年度版では，定性的であったカテゴリーに危険側故障平均時間などの確率論のファクターが追加され PL（Performance Level）と改訂された。PL のレベルは，a（低）～ e（高）の５段階となっている。

(2)　IEC 60204-1

機械制御盤の規格で，個々の部品への要求事項や**図６**で示すような部品の相互関係を示している。機械系の安全は，固有機械の規格を除きこの規格に準拠する必要がある。

(3)　IEC 61508

機械装置を安全な状態に維持するための“機能”を実装した E/E/PE（電気/電子/プログラマブル電子）機器の製品安全を規定しており，インバータ，電子制御機器，PLC が該当する。本規格を基に上記の機器の個別規格が制定されつつある。

4.2　機械の電気装置の安全構築

図７に，機械装置制御盤の安全システム例を示す。この図で示す制御盤を構成する部品は，**表１**の安全要求事項を満足する必要がある。特に主回路系の電気品や非常停止に関係する電気品は，従来要求されない規定が要求事項としてあることに注意が必要である。

富士電機では，この要求事項に対応するために原則として標準品に安全機能を取り入れた商品をラインアップしている。

5　機能安全への取組み

PA において，安全計装ループを構築する場合，多くの計測機器（圧力・差圧発信器）や安全コントローラ，安全 I/O を使う必要が出てくる。これらの機器は，機能安全規格（IEC 61508）に従った開発がなされ，第三者認証機関により安全に関して認証されたものでなければならない。富士電機では，①圧力・差圧発信器として「FCX-AⅡ/CⅡシリーズ」，②安全コントローラ，および安全 I/O として「MICREX-NX」を発売しており，“機能安全”の取組みを図っている。

本章では，その例として MICREX-NX で実現する安全計装システムについて紹介する。

5.1　安全計装システムに関する規格

安全計装システムに関係する規格には，IEC 61508 と IEC 61511 の二つがある。この二つの規格の違いは，IEC 61508 がデバイスの製造者・供給者を対象にし，IEC 61511 がシステムの設計者・インテグレータ・ユーザーを対象にしていることである。安全計装システムを設置する際には IEC 61511 に準拠する必要がある。

さらに，**図８**で示すシステム全体の安全ライフサイクル（計画・設計・設置・運転・改修・廃棄）も詳細に規定さ

れている。国内では，IEC 61508 の対応規格がすでに JIS で制定されており，IEC 61511 の対応規格も 2008 年 2 月に JIS で制定された。

特集

図 8　Total Safety（IEC 61508：E/E/EP 安全系）

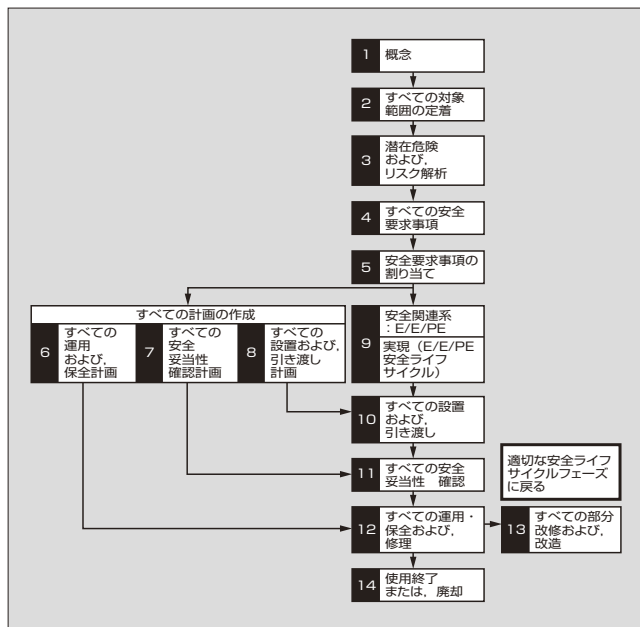



図 9　TÜV 認証証書

5.2　安全計装システム[2]

安全計装システム（SIS：Safety Instrumented System）は，プラント異常時のリスクを許容範囲以下に抑え，人命・環境・設備に対して高い安全性を確保する手段として必要なシステムである。従来，わが国ではリレー回路によるSIS が一般的であったが，欧米では新しい安全規格に準拠したコントローラを使った SIS が普及している。

(1)　ハードウェアとソフトウェア[3]

(a)　安全コントローラ

MICREX-NX で実現する SIS について説明する。MICREX-NX は，IEC 61508 に準拠し，第三者認証機関である TÜV（Technischer Überwachungs-Verein：技術検査協会）から安全度水準 SIL（Safety Integrity Level）3 の認証（**図 9**）を取得したコントローラである（134 ページの「解説」参照）。MICREX-NX で使用する CPU は処理能力の異なる 3 種類（AS412，AS414，AS417）を用意し，かつ，シングル構成から完全冗長化まで豊富なバリエーションで柔軟なシステム構成を可能としている。その結果，顧客システムの規模や用途によってシステム方式を選択できる拡張性を持っている（**表 2**）。大きな特徴として，一つの CPU（シングル構成）で SIL3 を実現していることである。これは，一つの CPU 内で二つのプログラムロジックが実行され，演算結果から CPU の健全性をチェックすることが可能な

図 10　CPU の健全性チェック

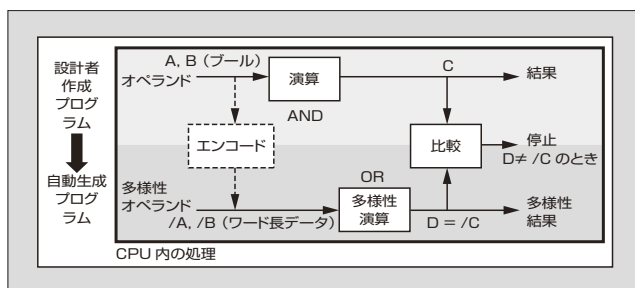



表 2　柔軟なシステム構成

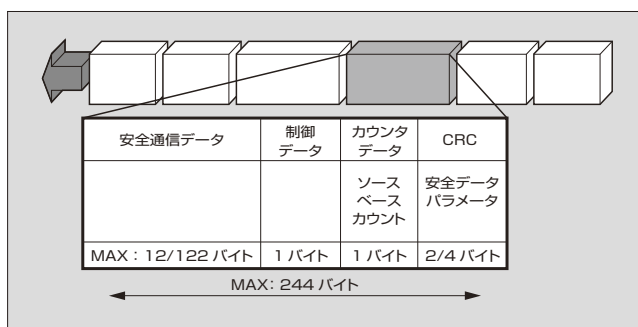
シングル構成	CPU，バス冗長化構成	CPU，バス，I/O冗長化構成
シングル構成でSIL3の安全水準を実現	CPU，バスの故障時もシステムを停止させることなく交換が可能	CPU，バスに加えI/Oの故障時もシステムを停止させることなく交換が可能

表 3　安全I/O

モジュール種別	入出力点数と安全レベル	電圧/電流仕様	設置環境
Digital input (DI 24)	24点：SIL2 AK4 12点：SIL3 AK6 (6点/コモン×4)	DC24 V	温度 水平取付：0～40℃ 垂直取付：0～60℃ 汚染環境 硫化水素H_2S：0.5 ppm以下 二酸化硫黄SO_2：0.1 ppm以下
Digital input (DI 8 NAMUR)	8点：SIL2 AK4 4点：SIL3 AK6	DC24 V	
Digital output (DO 10)	10点：SIL2 AK5 or SIL3 AK6	DC24 V 2 A	
Analog input (AI 6)	6点：SIL2 AK4 6点：SIL3 AK6	4～20 mA 0～20 mA* 0～10 V*	

＊：Safetyモード使用時は，4～20 mAのみ

図 11　PROFIsafe 通信テレグラム

図 12　Safety Matrix の機能（エンジニアリング）

アーキテクチャとなっているためである（図10）。一つ目のプログラムは設計者が作成したものであるが，二つ目のプログラムは，一つ目のプログラムがコンパイルされ実行形式に変換される際に，システムが自動生成した逆ロジックのプログラムである。CPU 内には自己診断機能が搭載されており，電源投入時，システム動作時に異常が検出された段階でシステムが安全方向に働く指示をする。また，接続されている I/O の異常や配線の断線などを検出することが可能である。

(b)　安全 I/O

安全 I/O の種類を表 3 に示す。各 I/O もまた，SIL3 の認証を取得している。I/O 内部の二つの CPU で二重化入力信号，出力信号の妥当性チェックを行い，また自己診断回路によるクロスチェックにより安全度を高めている。

(c)　安全通信

安全コントローラと安全 I/O の間は，PROFIBUS-DP をベースとした PROFIsafe プロファイルを使うことで安全通信を実現している[(4)]。PROFIsafe は IEC 61508 に準拠した最初の通信システムである。安全レベルは SIL3 に適合し FA，PA の広範囲な分野に適用可能である。PROFIsafe の通信テレグラムは図11のとおりで，PROFIsafe プロファイルでは，安全 I/O の信号データの後ろに，制御データ，カウンタデータ，CRC（Cyclic Redundancy Check）データを付加し，安全通信データの欠落を防いでいる。

(d)　エンジニアリング

安全制御プログラムのエンジニアリングは，専用のセーフティ関数ファンクションブロック（FB）（50 種類）を使用して行う。このセーフティ関数 FB は第三者認証機関 TÜV の認証を受けている。

エンジニアリング画面上に必要な FB を置き，それらをマウスで結線し，コンパイルすることで安全制御データ形式に変換される。エンジニアリング時には，画面を開く際やローディングする際にパスワードを要求され，決められた設計者だけがソフトウェアの設計や変更をすることができる。このように，不用意に安全プログラムが改変されないようセキュリティが考慮されている。

(2)　Safety Matrix

MICREX-NX には，「Safety Matrix」というソフトウェアが用意されている。この Safety Matrix は，大きく三つの機能を持っている（図12）。一つ目は，安全回路の自動生成機能である。Safety Matrix 上で，横軸に異常状態である信号を定義し，縦軸に安全動作をさせたい機器への出力信号を定義する。交差する点に対して関連づけを行うことで容易に安全プログラムを作成できる。二つ目は，エンジニアリングで作成した Safety Matrix の情報をそのまま監視用画面にモニタリングさせる機能である。これにより，異常事象（どのような異常が起きて，何が止まったのか）への的確な対応をタイムリーにとることが可能となる。三つ目は，exida 社の「exSILentia」とのデータ連携を可能とする機能である[(5)]。exSILentia は SIS の作動要求あたりの機能失敗平均確率（PFD：Probability of Failure on

図 13　Safety Matrix の機能（ライフサイクル管理）

図 14　SIS と DCS の統合

Demand）の計算，SIL 解析などアセスメントに利用されるソフトウェアである。この exSILentia で作成したデータを Safety Matrix にインポートすることで，さらにエンジニアリング効率を向上できる。また，Safety Matrix は，IEC 61511 が規定している安全ライフサイクル管理の一部に適応させることができ，エンジニアリングから管理まで，幅広く適用することができる（**図13**）。

(3)　SIS と DCS の統合

SIS が計測している状態監視や，ソフトウェアエンジニアリングは，**図 14** に示すように DCS（Distributed Control System）と同じ装置を使用して行う。

(a)　状態監視

SIS が計測している状況の監視は，DCS の標準監視端末で行う。DCS と同じ監視端末ということは，以下のような利点がある。

○ 緊急時でも慌てずに確実に監視・操作が行える。
○ SIS 動作状態と制御システムの状況を同一画面で確認でき，プラントの状態を的確に把握できる。

(b)　エンジニアリング

SIS エンジニアリングは，DCS と同じ標準エンジニアリングステーション（ES：Engineering Station）を使って行う。エンジニアリングは，通常の DCS で使用する CFC（Continuous Function Chart）を使用して，同一の環境と手順で行える。つまり，二つのエンジニアリングを使い分ける必要がないので効率のよいエンジニアリングが可能となる。また，DCS 側と信号の受渡しを行う場合でも，専用のインタフェース関数 FB を使用することで，システムの違いを意識することなく SIS を構築できる。

6　あとがき

Total Safety を目指した富士電機の機械安全と機能安全への取組みについて紹介した。安全は，機械安全だけ，機能安全だけでは成り立たなく，その両方を取り入れ総合的にプラントや設備の安全を考慮する必要があると考えている。今後も，国際規格に準拠して安心できる安全を“Total Safety”ソリューションとして提供していく所存である。

参考文献

(1)　IEC.
http://www.iec.ch/（参照 2007-12-21）
(2)　長谷川正美．制御システムとの統合を目指した安全計装システム．計装．vol.49, no.11, 2006, p.48-54.
(3)　池田卓史ほか．生産を最適化する新情報制御システム <MICREX-NX>．計測技術．466, vol.35, no.9, 2007, p.16-17.
(4)　日本プロフィバス協会．
http://www.profibus.jp/index.htm（参照 2007-12-21）
(5)　exida 社．
http://www.exida.com/（参照 2007-12-21）